

United States Senate
WASHINGTON, DC 20510-3703

COMMITTEES:
COMMITTEE ON FINANCE
COMMITTEE ON BUDGET
COMMITTEE ON ENERGY & NATURAL RESOURCES
SELECT COMMITTEE ON INTELLIGENCE
JOINT COMMITTEE ON TAXATION

June 5, 2019

The Honorable William Barr
Attorney General
U.S. Department of Justice
950 Pennsylvania Avenue, NW
Washington, D.C. 20530

Dear Attorney General Barr:

I write to better understand the steps taken by the Department of Justice and its component agencies to protect U.S. government offensive cyber capabilities from loss or theft by hackers and hostile foreign intelligence services. Just as the American people expect the government to protect its nuclear, chemical and biological weapons, so too do Americans expect that the government will protect its cyber arsenal from theft by hackers and foreign spies.

Several agencies within the Department of Justice have publicly acknowledged their use of offensive cyber capabilities, such as malware and so-called “zero-day” software tools that exploit cybersecurity flaws that are not known to the creators of the software. Since 2015, the FBI has acknowledged that it exploits zero-day flaws. The Drug Enforcement Administration revealed in a letter to Senator Grassley in 2015 that it had spent over \$900,000 to purchase a “tool that would allow for remote, overseas deployment of communications monitoring software” from Hacking Team, an Italian surveillance software company. The FBI has also publicly confirmed that it exploited security vulnerabilities in the Firefox web browser, as part of a bulk-hacking operation in 2015 during which the agency delivered malware to over 8,000 computers, located in 120 countries, all of which were used by individuals who visited the same FBI-controlled contraband website on the Dark Web.

Most famously, in 2016, the FBI paid an unnamed company more than a million dollars for a hacking tool that enabled the FBI to decrypt data stored on the San Bernardino terrorist’s iPhone. However, the government’s use of advanced cyber-capabilities is not limited to extracting data from seized smartphones.

DOJ has acknowledged the dangerous nature of its cyber tools and the need to keep them out of the wrong hands. In a criminal case in 2016, DOJ asked the court not to require it to provide a defendant, as part of the discovery process, with the web browser exploit that the FBI used to identify him. The court agreed with DOJ, finding that “the risk that the [browser exploit] might inadvertently be leaked or otherwise used by third parties is too great” and as a result, “the public should not bear this risk.”

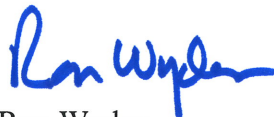
DOJ has also revealed that the companies that supply the government with hacking tools are a soft target for “attacks and infiltration by hostile entities wishing to exploit the technology they

provided to the FBI.” DOJ revealed this information as part of a federal lawsuit in 2017 in which the press sought information about the company that sold the FBI a tool to break into the San Bernardino terrorist’s iPhone. The FBI acknowledged that “the vendor likely does not have the same resources to devote to its own security [as the FBI]” and as such, “[i]t is reasonable to conclude that they would not be able to thwart the same types of attacks and infiltration attempts the FBI is currently able to defend against.” To that end, please provide me with responses to the following questions by July 12, 2019:

1. Has the Department of Justice and its component agencies ever had one of their offensive cyber capabilities “fall into the wrong hands,” such as through a breach or by being discovered “in the wild” by a target, cybersecurity researchers, or a foreign government? If yes, please describe whether that capability was subsequently abused to exploit U.S. government or private sector computer systems and provide an estimate of the damage caused.
2. Have any of the offensive cyber capabilities acquired from the private sector by the Department of Justice and its component agencies been developed by foreign companies? Has the Department of Justice or its component agencies audited these cyber capabilities to determine whether they “call home” to servers that are controlled by that company or are located outside the United States? If no, please explain why not.
3. Does the Department of Justice and its component agencies require that private sector suppliers of offensive cyber capabilities to the government:
 - a. Implement the National Institute for Standards and Technology Cybersecurity Framework? If no, please explain why not.
 - b. Adopt the cyber-security best practices that the Department of Homeland Security requires of federal civilian agencies and that are published at <https://cyber.dhs.gov>? If no, please explain why not.
 - c. Be subjected to “red team” cyber-security audits in order to discover whether non-public offensive cyber capabilities stored by the suppliers are sufficiently secure from hackers and foreign governments? If no, please explain why not.

Thank you for your attention to this serious matter.

Sincerely,



Ron Wyden
United States Senator